REVUE LAMY
RLDI
COLLECTION LAMY

DROIT DE L'IMMATÉRIEL

INFORMATIQUE MÉDIAS COMMUNICATION

LE NOUVEAU CADRE DE LA RÉSOLUTION EN LIGNE DES LITIGES DE CONSOMMATION AU SEIN DE L'UNION EUROPÉENNE : VERS UN MODE APPROPRIÉ DE RÉSOLUTION DES CONFLITS ?

Par Romain V. GOLA

104
MENSUEL
Mai
2014

Éclairages

9 *Cybersquatting* de noms de domaine : pourquoi et comment les stratégies de protection sont-elles amenées à évoluer ?
Par Nathalie DREYFUS

13 Filtrage de l'accès à un site contrefaisant (...)
Par Emmanuel DERIEUX

29 Analyse de la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation (...)
Par Myriam QUÉMÉNER

40 Affaires *Demanderjustice.com* : feu vert pour la dématérialisation des petits dossiers judiciaires ?
Par Éric LE QUELLENEC

Analyses

60 *Smart grid, compteurs intelligents* : « l'internet de l'énergie » au risque des données personnelles
Par David FOREST et Henri LEBEN

Colloque

96 « Données personnelles : bilan de 1995 et réforme de 2014 ? »
Par Caroline LAVERDET

Wolters Kluwer
France

Données personnelles : bilan de 1995 et réforme de 2014 ?

Le 20 mars 2014 s'est tenu le colloque annuel du Centre d'études juridiques et économiques du multimédia (Céjem) de l'université Panthéon-Assas – Paris-II, intitulé « Données personnelles : bilan de 1995 et réforme de 2014 ? ».

C'est à un compte rendu très complet des différentes interventions que nous convie présentement Me Caroline Laverdet.

Par Caroline LAVERDET

Avocat à la Cour

➔RLDI 3481

Sous la présidence du professeur Jérôme PASSA (directeur du Céjem et des masters II Droit du multimédia et de l'informatique [DMI] et Droit de la communication de Paris-II), les différents intervenants ont dans un premier temps adopté une approche générale (I) de l'encadrement actuel et futur des données personnelles pour proposer au public dans un second temps une approche sectorielle de l'utilisation de ces données, notamment dans les domaines relatifs à la cybercriminalité, à la liberté d'expression, au secteur bancaire et à ceux des télécoms et de la santé.

I. – APPROCHE GÉNÉRALE DE L'ENCADREMENT ACTUEL ET FUTUR DES DONNÉES PERSONNELLES

Nathalie METALLINOS (avocat à la Cour et enseignante à Paris-II) s'est intéressée en premier lieu à la directive n° 95/46/CE sur la protection des données à caractère personnel et à son besoin de réforme. Si en 1995 la perspective était l'harmonisation pour faciliter les échanges entre les États membres, il a été rappelé que ce texte n'est pas resté centré sur l'Union européenne, et que très rapidement les pays de l'Espace économique européen ont appliqué cette réglementation.

La directive n° 95/46/CE a ainsi servi de modèle à d'autres pays, notamment à l'Amérique latine, sous l'influence de l'Espagne, ainsi qu'à l'Asie. Toutefois, du fait d'une mondialisation aujourd'hui accrue et du développement rapide des systèmes de surveillance, il est apparu nécessaire de faire évoluer les règles, notamment dans le domaine régalien. Le projet de règlement a donc vocation à remplacer les règles actuelles posées par la directive n° 95/46/CE. Les principaux éléments de la réforme tendent ainsi à une accentuation des obligations des responsables de traitement et des sous-traitants, à une simplification des formalités, à un durcissement des sanctions, à un renforcement des droits des personnes et à une extension du champ d'application territorial, permettant d'assujettir à cette réglementation une société qui n'est pas établie sur le sol de l'Union européenne mais qui utilise des moyens ou des équipements de l'Union européenne. Concernant le calendrier d'adoption de ce texte, Nathalie Metallinos a indiqué que le Conseil européen poursuivrait ses travaux jusqu'en juillet pour obtenir un accord sur le texte d'ici à la fin de l'année, rappelant la position néanmoins très clivée des États quant à l'idée même d'un règlement, et l'intense lobbying exercé sur cette réforme, avec déjà plus de 4 000 amendements déposés sur le projet de règlement.

La place des responsables de traitements, des délégués aux données et de l'autorité de contrôle a ensuite été envisagée par Sophie NERBONNE (directrice adjointe des affaires juridiques à la Commission nationale de l'informatique et des libertés).

La création d'un statut légal des sous-traitants a été décrite, ainsi que la logique nouvelle de l'accountability du responsable de traitement, qui nécessitera pour celui-ci d'être dans un processus de démonstration des mesures prises pour assurer le respect des dispositions légales en matière de données personnelles. L'idée étant de bâtir un système de corégulation avec les responsables de traitement, en raison des difficultés évidentes pour la Cnil d'être en relation avec tous ces responsables, d'où l'appui sur des réseaux et notamment sur les délégués à la protection des données, connus en France sous la dénomination de « correspondants informatique et libertés ».

La problématique de la compétence territoriale des autorités de contrôle a également été abordée. À titre d'exemple, la Cnil est aujourd'hui compétente si le responsable du traitement n'a pas d'établissement dans l'Union européenne mais des moyens de traitement en France. Avec la réforme, si le responsable du traitement n'a pas d'établissement dans l'Union européenne, la Cnil sera compétente lorsque les traitements de données personnelles seront liés à la fourniture de biens ou de services aux personnes résidant en France ou à l'observation du comportement de ces personnes. Enfin, Sophie Nerbonne a partagé un certain nombre de réflexions en vue d'une gouvernance décentralisée, telles que

l'organisation d'une coopération entre les autorités par la désignation d'une « autorité chef de file » en cas de traitements transnationaux, qui serait l'interlocuteur unique des entreprises et le coordinateur des autorités compétentes, ainsi que la mise en place d'un mécanisme de codécision. Ces perspectives auraient pour avantage de rendre conjointe la compétence des autorités nationales de contrôle à tous les stades de l'examen du traitement, d'offrir une meilleure lisibilité du dispositif d'encadrement des données personnelles et un accroissement de la sécurité juridique pour les entreprises et les citoyens.

Jérôme HUET (professeur émérite à Paris-II) a quant à lui évoqué la question du consentement des personnes concernées par le traitement de leurs données personnelles et le peu d'importance qui leur a été donné par la loi « Informatique et libertés » du 6 janvier 1978. Si cette loi ne les ignore pas, en prévoyant notamment un droit d'accès et de rectification, leur droit d'opposition reste « fantomatique » en raison de l'obligation d'avoir un intérêt légitime pour le faire valoir.

Le projet de règlement met désormais en vedette la notion de « *consentement* » en lui consacrant des dispositions spéciales, mais le rôle du consentement est somme toute assez restreint, puisqu'il s'efface si le traitement est nécessaire aux intérêts légitimes de l'organisation.

Au final, seules certaines données personnelles sensibles, relatives notamment aux origines raciales, à la santé, à la vie sexuelle ou à la religion, ne peuvent pas être traitées à moins que la personne concernée n'ait donné son consentement. De même, s'il est prévu que le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il y a un déséquilibre significatif entre la position de la personne concernée et celle du responsable du traitement, cette disposition apparaît superficielle, dès lors que la personne concernée par le traitement aura toujours une position insignifiante face à un géant de l'internet.

Concernant l'expression du consentement, celle-ci étant souvent numérique, le projet de règlement renforce l'obligation d'information des personnes lorsque les données sont collectées auprès d'elles. En revanche, lorsque les données ne sont pas collectées auprès des personnes, il est alors prévu que les mêmes informations doivent leur être données, non pas pour obtenir leur consentement mais pour les informer, ce qui semble « assez peu réaliste ».

Après avoir rappelé le caractère nettement secondaire que peut jouer le consentement dans les transferts internationaux, Jérôme Huet s'est également interrogé sur la question de la preuve du consentement. Si la charge de la preuve du consentement incombe au responsable, on peut en effet se demander où et comment sont stockés les consentements des personnes concernées dans cette « gigantesque mer de données personnelles ». En conclusion, si le projet de règlement souhaite donner au consentement une dimension assez spéciale, on peut toutefois se montrer dubitatif sur l'efficacité du consentement à protéger les données personnelles.

La quatrième intervention de la matinée a été menée par Éric CAPRIOLI (avocat à la Cour, vice-président de la FNTC et du Cesin, et enseignant à Paris-II), qui a abordé le thème de la sécurité des traitements et des échanges internationaux de données personnelles.

La sécurité et la confidentialité des données faisant naturellement partie des principes de protection des données, les problématiques spécifiques aux transferts de données ont été évoquées. Ainsi les transferts de données au titre d'exigences légales ou réglementaires, comme pour la procédure américaine de *Discovery*, ou encore les transferts de données vers des prestataires privés, par exemple de *cloud computing*, posent la question de l'ampleur du traitement de ces données et de leur localisation qui reste bien souvent inconnue. Il a ainsi été indiqué que le projet de règlement pose en son chapitre V un principe d'interdiction des transferts de données à caractère personnel vers des États tiers, sauf dérogations légales comme la poursuite d'un intérêt légitime par le responsable du traitement ou encore le consentement de la personne concernée, et sauf décision d'adéquation relative au niveau de protection offert par l'État en cause. Toutefois, certains pays comme la principauté de Monaco, adhérents à la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ne font pas l'objet d'une décision d'adéquation, cette dernière étant d'ailleurs largement remise en cause par le Parlement européen.

En revanche, selon Éric Caprioli, l'apparition dans le projet de règlement de la responsabilité du sous-traitant est une avancée majeure, bien qu'elle soit limitée par l'absence de prise en compte des propres sous-traitants des sous-traitants des responsables de traitements, ce qui est pourtant aujourd'hui une réalité.

Enfin, les enjeux du principe d'*accountability* ont également été décrits, appelant la mise en œuvre de mesures techniques et organisationnelles adéquates et démontrables, l'établissement d'une politique de sécurité des traitements, notamment au niveau de l'intégrité et de la disponibilité des données, ainsi qu'une analyse d'impact préalable pour les traitements de données sensibles et une analyse des risques pour prendre les mesures les mieux adaptées. Ainsi, quelle que soit la situation, l'exportateur de données doit garantir la sécurité et la confidentialité des données.

Pierre LECLERCQ (conseiller honoraire à la Cour de cassation et ancien membre de la Cnil) a présidé la seconde partie du colloque, orientée vers une approche plus sectorielle du traitement des données personnelles (II).

II. – APPROCHE SECTORIELLE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Myriam QUÉMÉNER (avocat général près la Cour d'appel de Versailles) s'est préoccupée des problématiques liées aux données personnelles et à la cybercriminalité, estimant qu'il est moins risqué de commettre « un braquage numérique » qu'un braquage dans la vie réelle car il n'y a pas la confrontation directe entre l'auteur et la victime. Les infractions peuvent également être commises dans des « cyberparadis » où la législation est inexistante : si leurs effets se font ressentir en France, les enquêtes vont être complexifiées par les aspects liés à la réalisation d'investigations à l'étranger. On note parfois même un encouragement à la commission d'infractions sur internet, notamment par la création de pseudonymes. Les cyberdélinquants surfent ainsi sur l'actualité pour tenter d'escroquer les internautes par l'envoi de courriers électroniques, n'hésitant pas à reprendre les logos de sociétés connues pour rendre leurs e-mails plus crédibles afin que les internautes ne puissent pas distinguer le vrai du faux. Les données personnelles sont donc une manne pour

les délinquants, comme le montre le développement des faux profils sur Facebook ou les nombreuses tentatives de *phishing*. En outre, les délinquants sévissent de plus en plus sur des *darknets*, *via* notamment le réseau Tor, et cryptent leurs échanges, ce qui a pour conséquence de complexifier les enquêtes judiciaires. Le projet de règlement prévoit donc des sanctions plus lourdes en cas de violation de la confidentialité des données. Il inclut le droit à l'effacement des données, de nouvelles limites au « profilage », une pratique utilisée pour analyser ou prédire les performances professionnelles d'une personne, sa situation économique, sa localisation, etc., ou encore l'obligation d'utiliser un langage clair et simple pour expliquer les politiques sur le droit à la vie privée.

Par conséquent, les perspectives proposées par Myriam Quéméner s'orientent vers un développement de la formation pluridisciplinaire des acteurs et un renforcement de la coopération internationale. Il est en effet nécessaire de trouver un juste équilibre entre la protection de l'ordre public et celle des libertés individuelles.

Dans un second temps, Juliette MOREL-MAROGER (maître de conférences à l'université Paris-Dauphine) a envisagé les enjeux des traitements de données personnelles dans le secteur bancaire, traitements considérés comme indispensables à l'exercice de cette activité.

Si le concept de « *donnée bancaire* » ne figure pas en tant que telle dans les textes, il est possible de la définir de manière stricte comme tous les identifiants permettant de réaliser des opérations de banque (numéros de compte, etc.). Mais cette définition ne permet pas de traiter l'ensemble des problématiques posées par le traitement des données dans le secteur bancaire, les établissements de paiement traitant, par exemple, un très grand nombre de données sensibles qui peuvent être mutualisées entre les établissements appartenant à un même groupe ou encore exposées aux fraudes et aux falsifications. Le projet de règlement présente donc un certain nombre d'avancées dans le secteur bancaire, à savoir l'élargissement du champ d'application de la protection des données aux personnes morales, la généralisation du délégué à la protection des données personnelles, la communication aux victimes des violations de leurs données ainsi qu'un alourdissement des sanctions. Juliette Morel-Maroger a toutefois relevé que la protection offerte par le projet de règlement demeure incomplète et insuffisante, en raison de l'incertitude quant au champ d'application de la protection, du défaut d'exhaustivité de la protection, l'ensemble des traitements de données constitués dans le secteur bancaire n'étant pas concerné, et de l'inadaptation des modalités de la protection aux particularités du secteur bancaire. Les remèdes possibles seraient d'intégrer dans le chapitre IX du projet de règlement, qui concerne les situations particulières de traitements de données, un mécanisme propre à la matière bancaire, et de prévoir des garanties particulières en la matière, en raison du caractère intrusif des obligations imposées aux établissements bancaires.

Emmanuel DERIEUX (professeur à Paris-II) a quant à lui orienté son propos sur les relations entre la liberté d'expression et les données à caractère personnel.

Les médias sont en effet devenus d'importants pourvoyeurs et détenteurs de données personnelles, par la connexion des internautes aux réseaux de communication au public en ligne. La protection de ces données est donc une exigence pour la liberté d'expression, mais constitue également une limite à celle-ci : il est donc nécessaire de trouver un équilibre entre ces droits. L'orateur constate ainsi que la liberté d'expression est venue ces dernières années enrichir le volume des données personnelles. Dans les faits, chacun peut être émetteur de données personnelles en postant des messages sur des forums, des blogs ou des réseaux sociaux. En droit, la loi du 29 juillet 1881 « *sur la liberté de la presse* », la loi dite « *Informatique et libertés* » de 1978 et réformée en 2004, et la directive européenne n° 95/46/CE ont également renforcé l'exercice de la liberté d'expression. Mais la protection des personnes contribue parfois à restreindre la liberté d'expression. Le droit national et le droit européen posent ainsi un certain nombre de restrictions : on peut, par exemple, citer en droit interne les restrictions d'accès aux documents administratifs, la réglementation des archives, ainsi que les restrictions relatives au respect des personnes. Selon le professeur Derieux, la balance semble cependant pencher en faveur de la liberté d'expression. Mais aussi essentielle que soit celle-ci, la protection des données personnelles ne devrait-elle pas retenir la même attention ?

Le secteur des télécoms et les aspects relatifs aux réseaux sociaux ont par la suite été abordés par Marie-Gaëlle CHOISY (de la direction juridique du groupe Orange et correspondante informatique et libertés).

Les spécificités de ce secteur à forte mutation technologique et culturelle ont été rappelées, ainsi que sa richesse évidente en données personnelles. Celui-ci est réglementé par la directive sectorielle n° 97/66/CE, remplacée par la directive n° 2002/58/CE dite « *vie privée et communications électroniques* », qui ne s'applique qu'aux traitements de données personnelles effectués dans le cadre de la fourniture de services de communications et réglemente notamment les données de trafic, les données de géolocalisation, ainsi que la confidentialité des communications.

Dans un souci de renforcement des règles de sécurité, l'obligation de notifier toute violation des données personnelles auprès de la Cnil et auprès du particulier dont les données sont concernées par cette violation est étendue par le projet de règlement à l'ensemble des acteurs traitant des données personnelles (articles 30 à 32).

Concernant les réseaux sociaux, Marie-Gaëlle Choisy a rappelé que la plupart d'entre eux sont établis hors Union européenne, mais que leurs moyens de traitement peuvent être situés sur le territoire national. Les réseaux sociaux sont donc responsables des traitements, puisqu'ils déterminent les finalités et les moyens des traitements, indépendamment du fait qu'ils soient hébergeurs. Ils ont donc une obligation de sécurité au niveau des paramètres de confidentialité, notamment en ce qui concerne l'accès aux profils des utilisateurs. Toutefois, les responsabilités sont complexes puisque la détermination, sur ces réseaux, de la frontière entre groupe fermé et groupe ouvert est difficile.

Enfin, une dernière obligation pour les réseaux sociaux concerne le droit à l'oubli numérique et l'effacement des données. Le projet de règlement prévoit que le responsable du traitement doit informer la personne de l'effacement de ses données et faire en sorte que les tiers effacent tous les liens sur internet, ce qui semble particulièrement complexe à mettre en œuvre. Si le bilan de la directive n° 95/46/CE semble positif, le projet de règlement reprend ce bilan mais en le complexifiant, rendant ainsi son application difficile.

Le dernier thème, relatif aux données de santé, a été traité par Nathalie MARTIAL-BRAZ (professeur à l'université de Franche-Comté) et François MALYE (journaliste d'investigation au *Point*).

Ont été décrits les nouveaux enjeux à l'égard des données de santé, notamment économiques, en ce que les données de santé permettent de réaliser des profilages, de mettre en place des publicités ciblées, mais aussi de maîtriser le coût de la santé publique. La constitution de dossiers personnels de patients, tels que le DMP (dossier médical personnel) ou le dossier pharmaceutique, ainsi que le développement de la télémédecine et des nouvelles technologies au service de la santé (appli smartphone, puces RFID), nécessitent dès lors des garanties d'authentification du professionnel de santé comme du patient.

Les questions d'*open data* ont également été évoquées par Nathalie Martial-Braz qui a souligné la nécessité d'ouvrir ces bases de données pour la prévention des scandales sanitaires, la mise en place de politiques de soins, ainsi que le contrôle des politiques publiques et notamment des dépenses publiques de soins. Toutefois certains dangers liés au traitement de données sensibles et à l'utilisation des bases à des fins commerciales doivent être relevés. François Malye, auteur du classement annuel des hôpitaux et des cliniques de l'hebdomadaire *Le Point*, a partagé quant à lui son point de vue sur l'accès aux données de santé. Alors qu'une demande auprès de la Commission d'accès aux documents administratifs était auparavant nécessaire pour établir ce palmarès des hôpitaux, ces derniers se montrent désormais plus ouverts, en répondant à des questionnaires, dont les réponses sont couplées avec les données des recueils issus du programme de médicalisation des systèmes d'information (PMSI).

En conclusion du colloque annuel du Céjem, Jérôme Huet a souligné que le projet de règlement est pour une très grande part semblable au texte de la directive et qu'une directive aurait sûrement été préférable à un règlement, afin de laisser une certaine latitude aux États. Quant à la forme, Jérôme Huet considère en tout cas que le texte aurait dû se présenter comme une simple modification du précédent, sans changer les textes qui n'appelaient aucune retouche. Quant au fond, deux changements majeurs sont à retenir dans le projet de règlement : celui-ci se veut applicable non seulement si le traitement de données est réalisé dans un pays de l'Union européenne, mais aussi pour des traitements réalisés dans des pays tiers si des Européens sont ciblés par les traitements. Enfin, les sanctions prévues à l'encontre des responsables de traitement et notamment des grands groupes sont renforcées car des amendes proportionnelles au chiffre d'affaires des entreprises sont envisagées afin de lutter efficacement contre les traitements illicites de données à caractère personnel. ■